UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/002,064	10/31/2001	Richard L. Schertz	10017328-1	3568

7590 10/18/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 10/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/002,064	SCHERTZ ET AL.	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 July 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/31/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

RD

DETAILED ACTION

1. Applicant's arguments filed July 22, 2005, have been fully considered but they are not persuasive.

2. Claims 1-23 are pending and have been examined.

Response to Amendment

3. Regarding the Double Patenting rejection, Examiner directs Applicant's attention to pages 2-3 of the prior Office Action where Examiner specifically pointed out the claim language on each application that show the rejection is based on the claim language, not on the disclosure.

Examiner has rejected the claims based **solely** on the language found on the claims of the instant application and co-pending application.

Examiner was not mapping language found on the specification, but rather language found in the claims of the instant application to the language of the claims in the copending application.

The Double Patenting rejection **is not** withdrawn (emphasis added).

4. Examiner approves the amendment to the specification received on July 22, 2005. The objection to the specification is withdrawn.

5. Examiner approves the amendment to the drawings received on July 22, 2005. The objection to the drawings is withdrawn. The specific objection to reference character 18 being used for both "database" and "HTML" is also withdrawn.

6. The rejection under 35 U.S.C. 101 is withdrawn.

7. Regarding Applicant's argument that Maloney does not teach or suggest the claimed feature of "decoding the captured data from a first predetermined format to a second predetermined format decipherable by humans", Examiner has given the claims the broadest reasonable interpretation consistent with the specification, thus, a parsing tool to parse the data and make it available to an analytical engine for analyzing the data captured by the discovery tool clearly teach the claimed feature, as someone of ordinary skill in the art would. Furthermore, Maloney clearly refers to data on networks, packets that are analyzed to determine usage patterns and intrusion events (column 5, lines 1-67, column 11, lines 1-67, column 12, lines 1-42). Even assuming arguendo that Maloney does not "decode data to a second predetermined format **decipherable by humans**", the term/expression "decipherable by humans" is fairly broad, and does not specify what that format is. Some humans may feel more comfortable with certain "format" that other humans may find not "decipherable". Thus, given the claims the broadest reasonable interpretation consistent with the specification, Maloney does teach this feature.

Double Patenting

8. Claims 1-8, 9-18, and 20-23 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-8, 10-19, and 21-24 of copending Application No. 10/001,350. Although the conflicting claims are not identical, they are not patentably distinct from each other because the subject matter claimed in the instant application is fully disclosed in the referenced copending application.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

9. The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on that copending application since the referenced copending application and the instant application are claiming common subject matter, as follows: the copending application discloses a method of displaying data, comprising: capturing and decoding data, correlating data components, retrieving a web-browser template, and graphically displaying the correlated decoded data; the instant application discloses a method of displaying data, comprising: capturing and decoding data, correlating data components, and graphically displaying the correlated decoded data.

Claims 1-8, 9-18, and 20-23 of the instant application are envisioned by copending Application No. 10/001,350's claims 1-8, 10-19, and 21-24 in that claims 1-8, 10-19, and 21-24 of the copending application contain all the limitations of claims 1-8, 9-18, and 20-23 of the instant application. Claims 1-8, 9-18, and 20-23 of the instant application therefore are not patently distinct from the copending application claims and as such are unpatentable for obvious-type double patenting.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 5-9, 12-16, and 19-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maloney et al. (US Patent Number: 6,269,447), and further in view of Cooper et al. (US Publication Number: 2004/0103315).

Regarding claim 1, Maloney et al. teach a method of displaying data related to an intrusion event on a computer system, comprising: capturing data related to the intrusion event (column 4, lines 34-37); decoding the captured data from a first predetermined format to a second predetermined format decipherable by humans, the decoded data comprising data components of intrusion signature, data summary, and detailed data (column 4, lines 34-40); correlating data components of the intrusion signature, data summary and detailed data to one another (column 4, lines 53-60). Maloney et al. do not expressly disclose retrieving an web browser-based template; and graphically displaying the correlated decoded data components using the web browser-based template. Maloney et al. teach graphically displaying the correlated data components (column 4, lines 47-53), but are not specific as to using a browser. However, Cooper et al. teach retrieving an web browser-based template (page 5, paragraphs 88-90); and graphically displaying the correlated decoded data components using the web browser-based template (page 5, paragraphs 88-90). Therefore, it would

have been obvious to one having ordinary skill in the art at the time the invention was made to use web browser-based templates to graphically display correlated data. One of ordinary skill in the art would have been motivated to do so to provide an end user a tool to review reports from the end user's host computer as disclosed by Cooper et al. (page 2, paragraph 38, page 5, paragraph 90).

Regarding claim 5, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 1 above. Furthermore, Maloney et al. teach wherein capturing data comprises capturing network data packets of the intrusion event (column 4, lines 34-37, column 7, lines 23-27).

Regarding claim 6, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 1 above. Furthermore, Maloney et al. teach wherein decoding the captured data comprises decoding the captured data from a binary format to a human-readable text format (column 6, lines 8-20).

Regarding claim 7, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 1 above. Furthermore, Maloney et al. teach wherein decoding the captured data comprises decoding the captured data to decoded data having a data link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in hexadecimal format (column 4, lines 24-33, column 7, lines 65-67, column 8, lines 1-12).

Regarding claim 8, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 1 above. Furthermore, Maloney et al. teach wherein decoding the captured data comprises decoding the captured data to decoded

data having an Ethernet header, an IP header, an IP data summary, and packet data in hexadecimal format (column 4, lines 24-33, column 7, lines 65-67, column 8, lines 1-12).

Regarding claim 9, Maloney et al. teach a method of displaying data of an intrusion detection system, comprising: capturing, from a network, data related to an intrusion event in response to detecting an intrusion signature in the network data (column 4, lines 34-37); decoding the captured data from a predetermined format to a human-readable format, the decoded data comprising data components of network header data, data summary, and detailed data (column 4, lines 34-40); determining a correlation relationship between the data components of the intrusion signature, network header data, data summary and detailed data to one another (column 4, lines 53-60). Maloney et al. do not expressly disclose displaying the correlated decoded data components by using a web browser-based template. Maloney et al. teach graphically displaying the correlated data components (column 4, lines 47-53), but are not specific as to using a browser. However, Cooper et al. teach displaying the correlated decoded data components by using a web browser-based template (page 5, paragraphs 88-90). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use web browser-based templates to graphically display correlated data. One of ordinary skill in the art would have been motivated to do so to provide an end user a tool to review reports from the end user's host computer as disclosed by Cooper et al. (page 2, paragraph 38, page 5, paragraph 90).

Regarding claim 12, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 9 above. Furthermore, Maloney et al. teach wherein capturing data comprises capturing network data packets of the intrusion event in response to detecting the presence of a predetermined data pattern in the network data packet (column 4, lines 34-37, column 2, lines 23-33, column 12, lines 21-42).

Regarding claim 13, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 9 above. Furthermore, Maloney et al. teach wherein decoding the captured data comprises decoding the captured data from a binary format to a text format (column 6, lines 8-20).

Regarding claim 14, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 9 above. Furthermore, Maloney et al. teach wherein decoding the captured data comprises decoding the captured data to decoded data having a data link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in hexadecimal format (column 4, lines 24-33, column 7, lines 65-67, column 8, lines 1-12).

Regarding claim 15, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 9 above. Furthermore, Maloney et al. teach wherein decoding the captured data comprises decoding the captured data to decoded data having an Ethernet header, an IP header, an IP data summary, and packet data in hexadecimal format (column 4, lines 24-33, column 7, lines 65-67, column 8, lines 1-12).

Regarding claim 16, Maloney et al. teach a system of presenting data of an intrusion detection system, comprising: a network driver capturing data related to an intrusion event upon detecting a predetermined intrusion signature (column 7, lines 23-27, column 2, lines 23-33, column 12, lines 21-42); a decode engine decoding the captured data from a predetermined format to a predetermined format decipherable by humans, the decoded data comprising data components of intrusion event data, data summary, and detailed data (column 4, lines 34-40); and a user interface graphically correlating data components of the intrusion signature, intrusion event data, data summary and detailed data to one another (column 4, lines 53-60). Maloney et al. do not expressly disclose displaying the correlated decoded data components according to a web browser-based format. Maloney et al. teach graphically displaying the correlated data components (column 4, lines 47-53), but are not specific as to using a browser. However, Cooper et al. teach displaying the correlated decoded data components according to a web browser-based format (page 5, paragraphs 88-90). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use web browser-based templates to graphically display correlated data. One of ordinary skill in the art would have been motivated to do so to provide an end user a tool to review reports from the end user's host computer as disclosed by Cooper et al. (page 2, paragraph 38, page 5, paragraph 90).

Regarding claim 19, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 16 above. Furthermore, Cooper et al. teach the system, as set forth in claim 16, further comprising a web server operable to

transmit a file in a web-browser displayable format having the correlated and decoded data components (page 5, paragraph 90).

Regarding claim 20, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 16 above. Furthermore, Maloney et al. teach the system, as set forth in claim 16, wherein the network driver captures network data packets of the intrusion event in response to the intrusion detection system detecting a predetermined data pattern corresponding to the predetermined intrusion signature (column 7, lines 23-27, column 2, lines 23-33, column 12, lines 21-42).

Regarding claim 21, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 16 above. Furthermore, Maloney et al. teach the system, as set forth in claim 16, wherein the decode engine decodes the captured data from a binary format to a human-readable text format (column 6, lines 8-20).

Regarding claim 22, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 16 above. Furthermore, Maloney et al. teach the system, as set forth in claim 16, wherein the decode engine decodes the captured data to decoded data components having a data link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in hexadecimal format (column 4, lines 24-33, column 7, lines 65-67, column 8, lines 1-12).

Regarding claim 23, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 16 above. Furthermore, Maloney et al.

teach the system, as set forth in claim 16, wherein the decode engine decodes the captured data to decoded data components having an Ethernet header, an IP header, an IP data summary, and packet data in hexadecimal format (column 4, lines 24-33, column 7, lines 65-67, column 8, lines 1-12).

12. Claims 2-4, 10-11, and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maloney et al. and Cooper et al. as applied to claims 1, 9 respectively above, and further in view of Slodowski et al. (US Patent Number: 6,775,583).

Regarding claim 2, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 1 above. Maloney et al. and Cooper et al. do not disclose expressly graphically displaying the correlated decoded data components comprises graphically highlighting correlated data components of intrusion signature, data summary and detailed data. However, Slodowski et al. teach wherein graphically displaying the correlated decoded data components comprises graphically highlighting correlated data components of intrusion signature, data summary and detailed data (column 5, lines 13-43). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to graphically display data, highlighting correlated data. One of ordinary skill in the art would have been motivated to do so to provide users with an easy to learn, easy to handle, and comfortable data arrangement (Slodowski et al., column 2, lines 54-67).

Regarding claim 3, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 1 above. Maloney et al. and Cooper et al. do not

disclose expressly wherein graphically displaying the correlated decoded data components comprises: receiving a user input selecting a displayed data component; and graphically highlighting data components correlated to the selected data component. However, Slodowski et al. teach wherein graphically displaying the correlated decoded data components comprises: receiving a user input selecting a displayed data component; and graphically highlighting data components correlated to the selected data component using the web browser-based template (column 5, lines 13-43). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to graphically display data, highlighting correlated data. One of ordinary skill in the art would have been motivated to do so to provide users with an easy to learn, easy to handle, and comfortable data arrangement (Slodowski et al., column 2, lines 54-67).

Regarding claim 4, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 1 above. Maloney et al. and Cooper et al. do not disclose expressly wherein graphically displaying the correlated decoded data comprises: receiving a user input selecting a displayed data component; graphically highlighting the user selected data component using the web browser-based template; and graphically highlighting data components correlated to the selected data component using the web browser-based template. However, Slodowski et al. teach wherein graphically displaying the correlated decoded data comprises: receiving a user input selecting a displayed data component; graphically highlighting the user selected data component using the web browser-based template; and graphically highlighting data

components correlated to the selected data component using the web browser-based template (column 5, lines 13-43). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to graphically display data, highlighting correlated data. One of ordinary skill in the art would have been motivated to do so to provide users with an easy to learn, easy to handle, and comfortable data arrangement (Slodowski et al., column 2, lines 54-67).

Regarding claim 10, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 9 above. Maloney et al. and Cooper et al. do not disclose expressly wherein graphically displaying the correlated decoded data comprises: receiving a user input selecting a displayed data component; and graphically highlighting all data components correlated to the selected data component using an HTML template. However, Slodowski et al. teach wherein graphically displaying the correlated decoded data comprises: receiving a user input selecting a displayed data component; and graphically highlighting all data components correlated to the selected data component using an HTML template (column 5, lines 13-43). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to graphically display data, highlighting correlated data. One of ordinary skill in the art would have been motivated to do so to provide users with an easy to learn, easy to handle, and comfortable data arrangement (Slodowski et al., column 2, lines 54-67).

Regarding claim 11, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 9 above. Maloney et al. and Cooper et al. do not disclose expressly wherein graphically displaying the correlated decoded data

comprises: receiving a user input selecting a displayed data component; graphically highlighting the user selected data component; and graphically highlighting data components correlated to the selected data component. However, Slodowski et al. teach wherein graphically displaying the correlated decoded data comprises: receiving a user input selecting a displayed data component; graphically highlighting the user selected data component; and graphically highlighting data components correlated to the selected data component (column 5, lines 13-43). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to graphically display data, highlighting correlated data. One of ordinary skill in the art would have been motivated to do so to provide users with an easy to learn, easy to handle, and comfortable data arrangement (Slodowski et al., column 2, lines 54-67).

Regarding claim 17, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 16 above. Maloney et al. and Cooper et al. do not disclose expressly wherein the user interface graphically highlights correlated data components of intrusion event data, data summary and detailed data. However, Slodowski et al. teach wherein the user interface graphically highlights correlated data components of intrusion event data, data summary and detailed data (column 5, lines 13-43). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to graphically display data, highlighting correlated data. One of ordinary skill in the art would have been motivated to do so to provide users with an easy to learn, easy to handle, and comfortable data arrangement (Slodowski et al., column 2, lines 54-67).

Regarding claim 18, the combination of Maloney et al. and Cooper et al. teaches the limitations as set forth under claim 16 above. Maloney et al. and Cooper et al. do not disclose expressly wherein the user interface is operable to receive a user input selecting a displayed data component, and graphically highlights all data components correlated to the selected data component using a web-based display template. However, Slodowski et al. teach wherein the user interface is operable to receive a user input selecting a displayed data component, and graphically highlights all data components correlated to the selected data component using a web-based display template (column 5, lines 13-43). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to graphically display data, highlighting correlated data. One of ordinary skill in the art would have been motivated to do so to provide users with an easy to learn, easy to handle, and comfortable data arrangement (Slodowski et al., column 2, lines 54-67).

Conclusion

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100